บทวิจารณ์หนังสือ

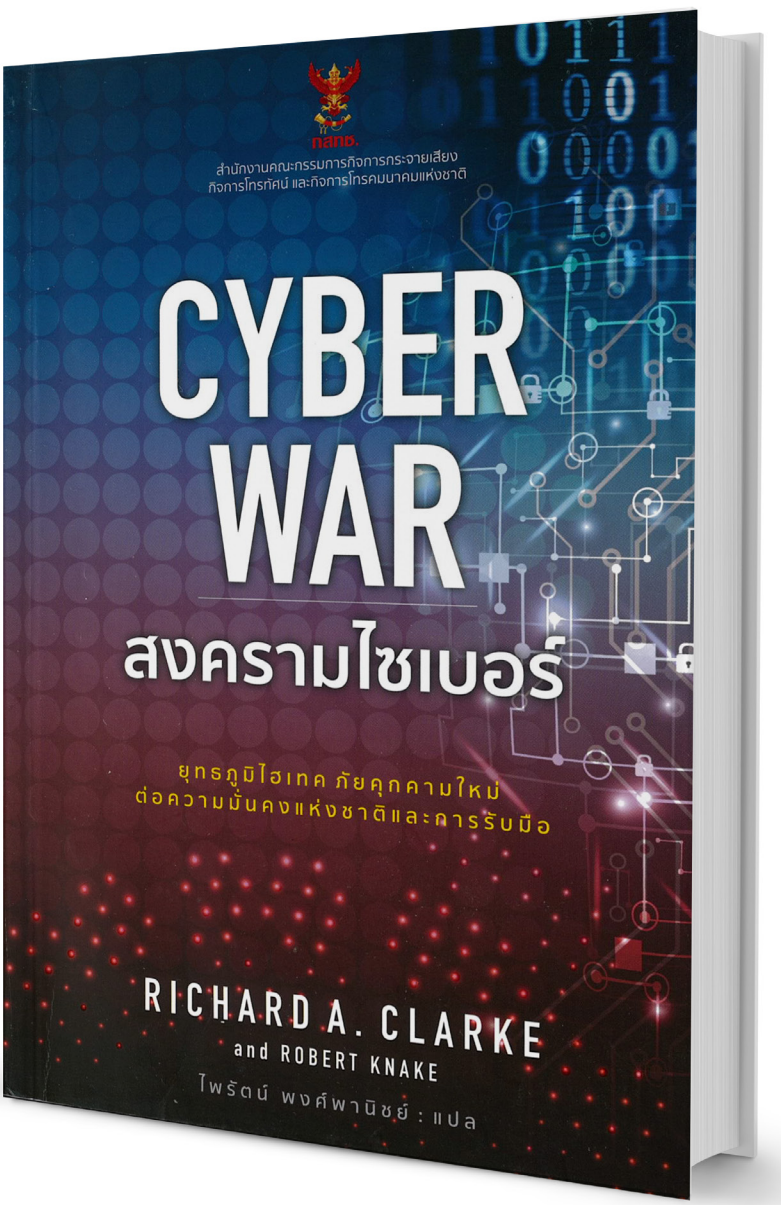
วิชัย โชควิวัฒน

Vichai Chokevivat

สถาบันวิจัยระบบสาธารณสุข นนทบุรี 11000

Health Systems Research Institute, Nonthaburi 11000 Thailand

Corresponding E-mail : vichaichok@yahoo.com


กสทช.
สำนักงานคณะกรรมการกิจการกระจายเสียง
กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ
CYBER
WAR
สงครามไซเบอร์
ยุทธภูมิไฮเทค ภัยคุกคามใหม่
ต่อความมั่นคงแห่งชาติและการรับมือ
RICHARD A. CLARKE
and ROBERT KNAKE
ไพรัตน์ พงศ์พานิชย์ : แปล

สงครามไซเบอร์
CYBER WAR

ไพรัตน์ พงศ์พานิชย์
แปลจาก Cyber War
by Richard A. Clarke and Robert Knake
สำนักพิมพ์มติชน พิมพ์ครั้งแรก กุมภาพันธ์ 2555
415 หน้า 250 บาท

หนังสือเล่มนี้เป็นอีกเล่มที่มีตราของสำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) พิมพ์อยู่บนหน้าปก แสดงถึงการสนับสนุนของ กสทช. ให้มีการแปลและพิมพ์เผยแพร่หนังสือเล่มนี้ในสังคมไทย บนปกหลังของหนังสือยังมีคำนิยมของ พล.อ.อ. ธเรศ ปุณศรี ประธาน กสทช. คนแรก ปรากฏอยู่ด้วย ซึ่งเป็นข้อเขียนสั้น ๆ แต่อธิบายเหตุผลของการเผยแพร่หนังสือนี้ไว้อย่างชัดเจนว่า

"ในขณะที่ความก้าวหน้าทางเทคโนโลยีของเครือข่ายอินเทอร์เน็ต ซึ่งเป็นตัวขับเคลื่อนสำคัญในโลกไซเบอร์ ก่อให้เกิดการสร้างสรรค์นวัตกรรมใหม่ ๆ เพื่อรองรับการใช้งานทั้งการดำเนินชีวิตประจำวันของมนุษย์ให้สามารถติดต่อสื่อสารและใช้งานอุปกรณ์สมัยใหม่ได้อย่างสะดวกสบาย ตลอดไปจนถึงการบริหารงานภาครัฐในยุคเศรษฐกิจดิจิทัลที่ทำให้การทำงานมีประสิทธิภาพสูงยิ่งขึ้น แต่ในขณะเดียวกันก็เป็นการเปิดโอกาสให้ผู้ไม่หวังดีได้ใช้ความก้าวหน้าของเทคโนโลยีนี้เพื่อเข้าถึงข้อมูลสำคัญของผู้ใช้งานซึ่งส่วนใหญ่ไม่ได้ระมัดระวังจึงไม่ตระหนักถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ดังกล่าวส่งผลให้เกิดการเสียหายได้ในที่สุด ในปัจจุบันทางการทหารได้จัดภัยคุกคามนี้ให้เป็นสงครามไซเบอร์ โดยกำหนดให้เป็นแนวรบที่ 5 (5th Domain) เพราะถือว่าเป็นอันตรายอย่างร้ายแรงต่อเสถียรภาพของประเทศเพราะมีเป้าหมายในการโจมตีทั้งทางด้านสังคม เศรษฐกิจ โครงสร้างพื้นฐาน และความมั่นคงของประเทศ ด้วยการโจมตีในหลายรูปแบบทั้งการโจรกรรมข้อมูล การโจมตีเว็บไซต์ การเจาะข้อมูลสำคัญและการทำลายระบบคอมพิวเตอร์ที่ควบคุมการทำงานของระบบสาธารณูปโภคหลัก ๆ เป็นต้น ซึ่งล้วนแต่สร้างความเสียหายต่อความมั่นคงของประเทศโดยรวมเป็นอย่างยิ่ง

กสทช. ตระหนักถึงภัยคุกคามทางไซเบอร์ที่กล่าวข้างต้น ที่ประเทศไทยจะต้องเผชิญในอนาคตอย่างที่มิอาจหลีกเลี่ยงได้ จึงเริ่มให้ความรู้เรื่องนี้ในรูปแบบต่าง ๆ เช่น การบรรยายโดยผู้เชี่ยวชาญ การสัมมนาและเลือกสรรหนังสือเกี่ยวกับภัยคุกคามทางไซเบอร์เพื่อให้ความรู้และแจกจ่ายให้กับภาครัฐ ภาคเอกชน และประชาชนผู้สนใจมาอย่างต่อเนื่อง”

เรื่องสงครามไซเบอร์เป็นเรื่องของความก้าวหน้าอย่างมากทางเทคโนโลยี และมีลักษณะเป็นนามธรรมสูง หนังสือเล่มนี้จึงมีความยากถึง 3 ระดับ **ระดับแรก** เป็นความยากของตัวระบบเอง เพราะเป็นเทคโนโลยีชั้นสูง มีความซับซ้อน และมีพัฒนาการรวดเร็วมาก ยากที่คนที่มิได้เรียนมาโดยตรง หรือมิได้ตั้งใจศึกษาอย่างจริงจังจะสามารถเข้าใจระบบและวิธีการทำงานของทั้งตัวเครื่องกลและเครือข่ายได้อย่างทะลุปรุโปร่ง ความยาก **ระดับที่สอง** ของหนังสือเล่มนี้ อยู่ที่เป็นเรื่องที่มุ่งเขียนสำหรับผู้มีอำนาจหน้าที่และผู้เกี่ยวข้องกับสังคมสหรัฐอเมริกา ซึ่งมีระบบการเมืองการปกครอง ระบบบริหาร พัฒนาการทางประวัติศาสตร์ วิธีคิด วัฒนธรรมการทำงาน และระดับความก้าวหน้าทางเทคโนโลยีด้านนี้แตกต่างจากบริบทในสังคมไทยมาก นอกจากนี้ยังมีความยาก**ระดับที่สาม** คือกำแพงทางภาษา ทั้งตัวศัพท์ทางเทคนิคในสาขาวิชาเองที่จำนวนมากยังไม่มีศัพท์บัญญัติภาษาไทย และแม้มีความพยายามเสนอศัพท์บางคำแต่อาจยังไม่เป็นที่ยอมรับ หรือยังไม่แพร่หลายชื่อองค์กรต่าง ๆ และคำอธิบาย สาระสำคัญจำนวนมาก ก็ยากในการถ่ายทอดเป็นภาษาไทยที่สละสลวยและเข้าใจง่าย แม้ผู้แปลหนังสือเล่มนี้จะเป็นผู้สนใจในแวดวงนี้ และมีผลงานแปลหนังสือในแนวนี้ออกมาบ้างแล้ว แต่โดยพื้นฐานการศึกษาทางสายสังคมศาสตร์ และไม่ได้มีโอกาสไปศึกษาในประเทศที่ใช้ภาษาอังกฤษอย่างสหรัฐอเมริกา จึงทำให้มีข้อจำกัดไม่น้อยในการที่จะถ่ายทอดเนื้อหาข้ามศาสตร์ และข้ามวัฒนธรรมออกมา บรรณาธิการหนังสือเล่มนี้เป็นนักเขียนนักแปลมีชื่อ แต่ก็ไม่ได้อยู่ในแวดวงของศาสตร์แขนงนี้โดยตรง

จุดเด่นของหนังสือเล่มนี้อยู่ที่ผู้เขียนหลักคือ ริชาร์ด เอ. คลาร์ก ซึ่งเป็นผู้เชี่ยวชาญด้านความมั่นคงระดับสูงของสหรัฐอเมริกา และมีประสบการณ์เป็นที่ปรึกษาด้านความมั่นคงของประธานาธิบดีสหรัฐถึง 4 คน คือ โรนัลด์ เรแกน บุช ทั้งพ่อและลูก และบิลล์ คลินตัน ขณะเขียนหนังสือเล่มนี้ยังเป็นอาจารย์ที่สำนักวิชารัฐประศาสนศาสตร์เคนเนดี มหาวิทยาลัยฮาร์วาร์ด และยังเป็นที่ปรึกษาให้กับสำนักข่าวเอบีซีนิวส์ และประธานที่ปรึกษาของบริษัทด้านให้คำปรึกษาเอกชน รวมทั้งยังมีประสบการณ์การเขียนหนังสือขายดีมาแล้วด้วย

นอกจากความรู้และประสบการณ์สูงยิ่งของผู้เขียนแล้ว หนังสือนี้ยังมีผู้เขียนร่วมคือ โรเบิต คเนค ซึ่งเรียนจบมาโดยตรงในระดับปริญญาโทด้านความมั่นคงระหว่างประเทศ จากสำนักวิชารัฐประศาสนศาสตร์เคนเนดี มหาวิทยาลัยฮาร์วาร์ด เป็นนักวิชาการด้านกิจการระหว่างประเทศอยู่ที่สภาวิเทศสัมพันธ์ และมีงานเขียนด้านความมั่นคงให้แก่สื่อสิ่งพิมพ์ต่าง ๆ หลายฉบับ

โดยที่เรื่องสงครามไซเบอร์เป็นเรื่องเข้าใจยากและซับซ้อน แต่หนังสือนี้ก็เขียนขึ้นอย่างมืออาชีพ โดยแบ่งเนื้อหาเป็น 8 บท เริ่มจากบทโหมโรง ต่อด้วยเรื่องขุนศึกไซเบอร์ สมรภูมิ เมื่อการป้องกันล้มเหลว ก้าวสู่ยุทธศาสตร์ป้องกัน จะรุกอย่างไร สันติภาพไซเบอร์ และจบลงด้วยข้อเสนอสำหรับระเบียบวาระแห่งชาติ รวม 6 ข้อ

หนังสือพยายามคลี่คลายความซับซ้อนโดยมีการเปรียบเทียบกับเรื่องที่เป็นรูปธรรม คือ เรื่อง สงครามในอดีตต่าง ๆ ทั้งสงครามเย็น สงครามร้อน และภัยสงครามนิวเคลียร์ มีการหยิบยกเหตุการณ์จริงของการรบในอดีตมาเชื่อมโยง โดยการเขียนทั้งเรื่องราวที่ปรากฏในประวัติศาสตร์ หรือเรื่องราวที่ปรากฏในสื่อต่าง ๆ อย่างกว้างขวาง รวมทั้งประสบการณ์ตรงของผู้เขียนมานำเสนอไว้อย่างน่าติดตาม จะขอยกตัวอย่างรูปธรรมมากล่าวถึงเพียง 2 เรื่อง

เรื่องแรก อยู่ในบทโหมโรง มีการเล่าถึงเหตุการณ์วันที่ 6 กันยายน พ.ศ. 2550 ที่อิสราเอลส่งเครื่องบินเอฟ-15 อีเกิล และ เอฟ-16 ฟัลคอน เข้าไประเบิดทำลายอาคารแห่งหนึ่งในซีเรีย ซึ่งก่อสร้างโดยคนงานจากเกาหลีเหนือ และเชื่อว่าเป็นโรงงานผลิตอาวุธนิวเคลียร์ที่ออกแบบโดยเกาหลีเหนือ การทำลายประสบความสำเร็จอย่างดี ทั้ง ๆ ที่เป็นปฏิบัติการในดินแดนของอีกประเทศหนึ่ง โดยระบบเรดาร์ในพื้นที่ถูกทำให้ “เดี้ยง” ไปก่อน จึงไม่มีการป้องกันหรือต่อต้านใด ๆ นี่คือ “สงครามไซเบอร์” ซึ่งนิยามเบื้องต้นเขียนไว้ในบทโหมโรงว่าหมายถึง “การดำเนินการโดยรัฐชาติหนึ่งเพื่อแทรกซึมคอมพิวเตอร์หรือเครือข่ายของอีกรัฐชาติหนึ่งเพื่อวัตถุประสงค์ในการก่อให้เกิดความเสียหาย หรือการรบกวนขัดขวางกระบวนการดำเนินการตามปกติให้หยุดชะงัก” ทั้งนี้เมื่ออิสราเอลโจมตีซีเรีย พวกเขาได้ใช้ลำแสงแรงดันไฟฟ้า ไม่ใช่เพื่อการตัดเหมือนมีดเลเซอร์ หรือเพื่อทำให้หมดสติเหมือนปืนเทเซอร์ (ปืนช็อตไฟฟ้า) แต่เพื่อใช้ในการส่งข้อมูลที่ประกอบด้วยเลขฐาน 2 คือ 1 และ 0 สำหรับใช้ในการควบคุมสิ่งที่เรดาร์ในระบบป้องกันทางอากาศของซีเรียให้หมดสภาพ ใช้การไม่ได้ แทนที่จะระเบิดเรดาร์ให้กระจุยกระจายไปก่อนที่จะบุกถล่มเป้าหมายหลักได้อย่างง่ายดาย

นี่คือตัวอย่างเล็ก ๆ ของสงครามไซเบอร์ สำหรับในระดับใหญ่กว่านั้น มีสรุปไว้สั้น ๆ ในคำนำของสำนักพิมพ์ในหนังสือเล่มนี้ นั่นคือ “ประเทศใดประเทศหนึ่งอาจจะทำให้ระบบสั่งการทางทหารของประเทศที่เป็นเป้าหมายโจมตีเป็นง่อยได้ ทำให้ระบบการเงิน ระบบสาธารณูปโภค ไฟฟ้า ประปา หรือขนส่งมวลชนของประเทศที่เป็นเป้าหมายไม่สามารถทำงานได้ เพียงแค่เคาะแป้นคีย์บอร์ดคอมพิวเตอร์เท่านั้น”

ทั้งนี้ คีย์บอร์ดที่เคาะจะอยู่ที่ไหนก็ได้ ไม่จำเป็นต้องอยู่ในดินแดนประเทศตรงข้าม

เรื่องที่สอง เป็นคำอธิบายว่าทำไมและอย่างไรสงครามไซเบอร์จึงเป็นไปได้ ซึ่งเขียนไว้ในบทที่สาม ซึ่งสรุปว่าอินเทอร์เน็ตนั้นมีความเปราะบางอย่างน้อย 5 ประการที่ทำให้นักรบไซเบอร์เจาะเข้าสู่ระบบและทำการทำลายล้างได้ ได้แก่ (1) เพราะระบบอินเทอร์เน็ตเชื่อมโยงกันทั่วโลก โดยระบบที่สร้างขึ้น “ถูกออกแบบมาโดยคำนึงถึงความปลอดภัยน้อยมาก” (2) จุดเชื่อมต่อระหว่างผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider : ISP) เป็นอีกจุดที่ถูกโจมตีได้โดยง่าย เพราะไม่มีผู้ควบคุมบริหาร ณ จุดดังกล่าว โดยในช่วงเริ่มแรกของการพัฒนาระบบอินเทอร์เน็ตโดย “องค์การการวิจัยชั้นสูง” (Advanced Research Project Agency : ARPA) ของกระทรวงกลาโหมสหรัฐ ทำหน้าที่บริหารเครือข่ายนี้ ต่อมา “บรรษัทอินเทอร์เน็ตเพื่อกำหนดชื่อและหมายเลข” (Internet Corporation for Assigned Names and Numbers : ICANN) เข้ามาทำหน้าที่ดูแลเฉพาะเรื่องชื่อและหมายเลขเท่านั้น (3) เกือบทุกอย่างที่ทำให้อินเทอร์เน็ตทำงานได้ผลนั้นเปิดกว้าง ไม่มีการเข้ารหัส จึงเปิดกว้างสำหรับนักรบไซเบอร์ด้วย (4) ความสามารถของอินเทอร์เน็ตเองในการแพร่” มัลแวร์ออกไปในวงกว้าง และ (5) ความใหญ่โตมโหฬารของระบบอินเทอร์เน็ตที่ถูกออกแบบมาให้ไม่สามารถรวมศูนย์ได้ จุดเปราะบางทั้ง 5 ประการคือ ช่องทางที่นักรบไซเบอร์สามารถเลือกเจาะเข้าสู่ระบบได้ทั้งสิ้น

หนังสือเล่มนี้เสนอเรื่องสำคัญที่สุดสำหรับผู้บริหารไว้ในบทสุดท้าย ซึ่งมีชื่อบทว่า “ระเบียบวาระแห่งชาติ” ซึ่งมีการเสนอไว้รวม 6 ระเบียบวาระ ได้แก่ (1) ให้ “คำนึงถึงเรื่องที่มองไม่เห็น” คือตระหนักถึงความสำคัญของสงครามไซเบอร์ (2) วาง “แนวป้องกันหลัก 3 ทาง” “เพื่อที่จะให้ชาติอื่นต้องใคร่ครวญซ้ำสองก่อนจะลงมือเปิดสงครามไซเบอร์กับเรา” (3) ต้องมุ่งลด “อาชญากรรมไซเบอร์” ด้วยการแก้ปัญหาความ “ไม่ประสีประสาทางคอมพิวเตอร์” ของเจ้าหน้าที่ที่มีอำนาจหน้าที่ต่าง ๆ (4) ต้องสนับสนุนให้เกิดข้อตกลงที่มีผลเหมือน “สนธิสัญญาจำกัดอาวุธทางยุทธศาสตร์” (Strategic Arms Limitation Treaty : SALT) ที่ได้ผลดีในการจำกัดอาวุธนิวเคลียร์มาแล้ว (5) ต้องวิจัยและพัฒนาเครือข่ายไซเบอร์ให้ดีขึ้นกว่าเดิม เพราะระบบอินเทอร์เน็ต มีอายุย่างเข้า “วัยกลางคน” หรือวัยสูงอายุแล้ว และ (6) การตัดสินใจที่สำคัญสุดท้ายต้องอยู่ที่ผู้นำสูงสุดของประเทศ คือ ประธานาธิบดี

หนังสือเล่มนี้เขียนมาตั้งแต่ พ.ศ. 2553 แปลและพิมพ์เผยแพร่เป็นภาษาไทย เมื่อ พ.ศ. 2555 แต่ดังที่ พล.อ.อ. ธเรศ ปุณศรี ได้เขียนไว้ในคำนิยมว่า “ยังมีเนื้อหาที่นำมาประยุกต์ใช้ได้ในปัจจุบัน เพราะมีสาระอันเป็นประโยชน์ และมีตัวอย่างเหตุการณ์สำคัญที่เกิดขึ้นในอดีต จะช่วยให้ผู้อ่านที่ปฏิบัติงานในหน่วยงานภาครัฐ ภาคเอกชน และประชาชนทั่วไป ได้ตระหนักถึงความสำคัญและเข้าใจได้ว่าอะไรคือสงครามไซเบอร์ เกิดขึ้นได้อย่างไร และเตรียมตัวรับมือกับภัยคุกคามเหล่านี้ในโลกยุคดิจิทัลที่ทุกคนต้องพึ่งพาอินเทอร์เน็ตมากขึ้นทุกวัน”